Secure Internet Commerce - Design and Implementation of the Security Architecture of Security First Network Bank, FSB

Nicolas Hammond

NJH Security Consulting

njh@njh.com

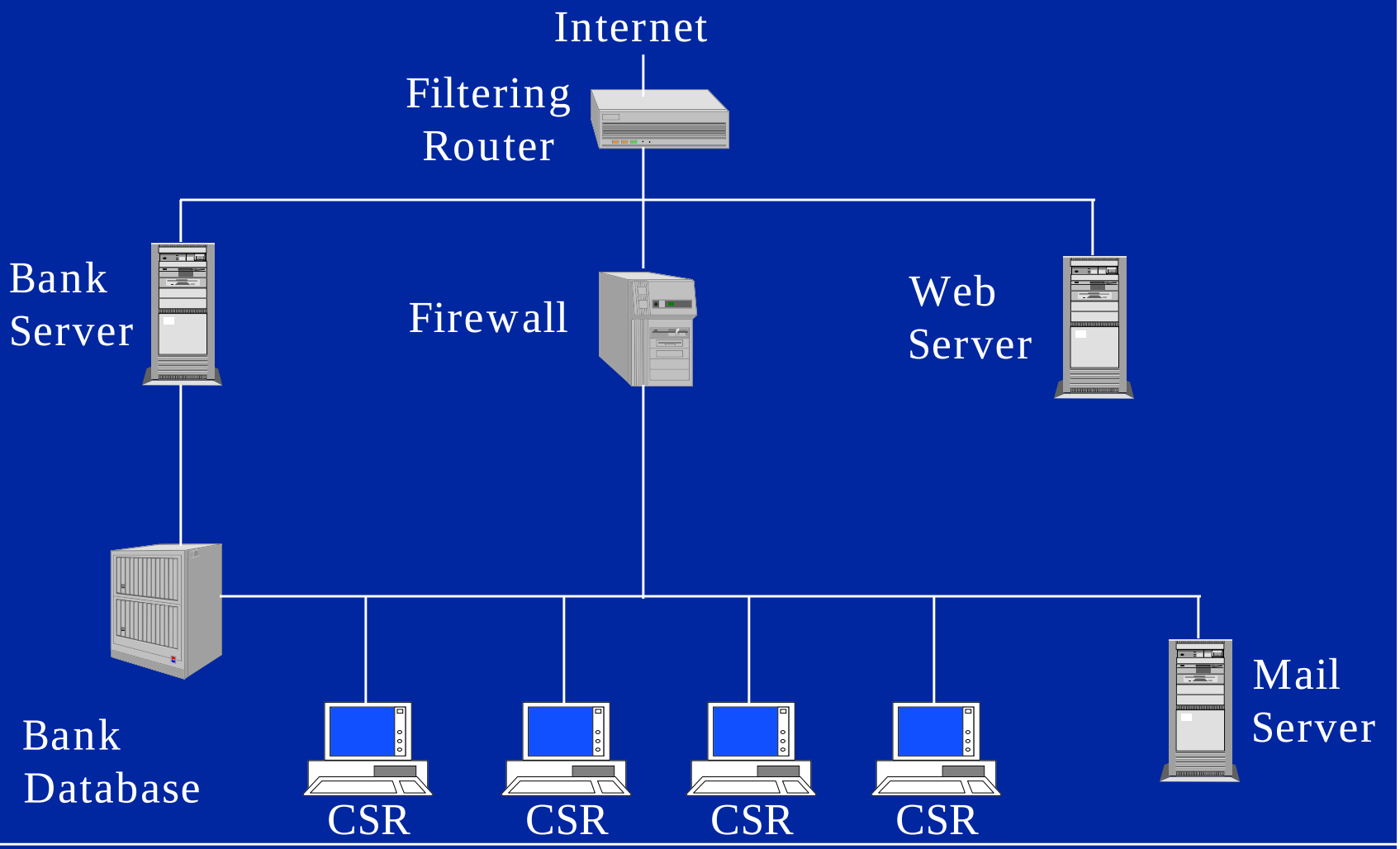
http://www.njh.com

Tel: 404-262-1633 Fax: 404-812-1984

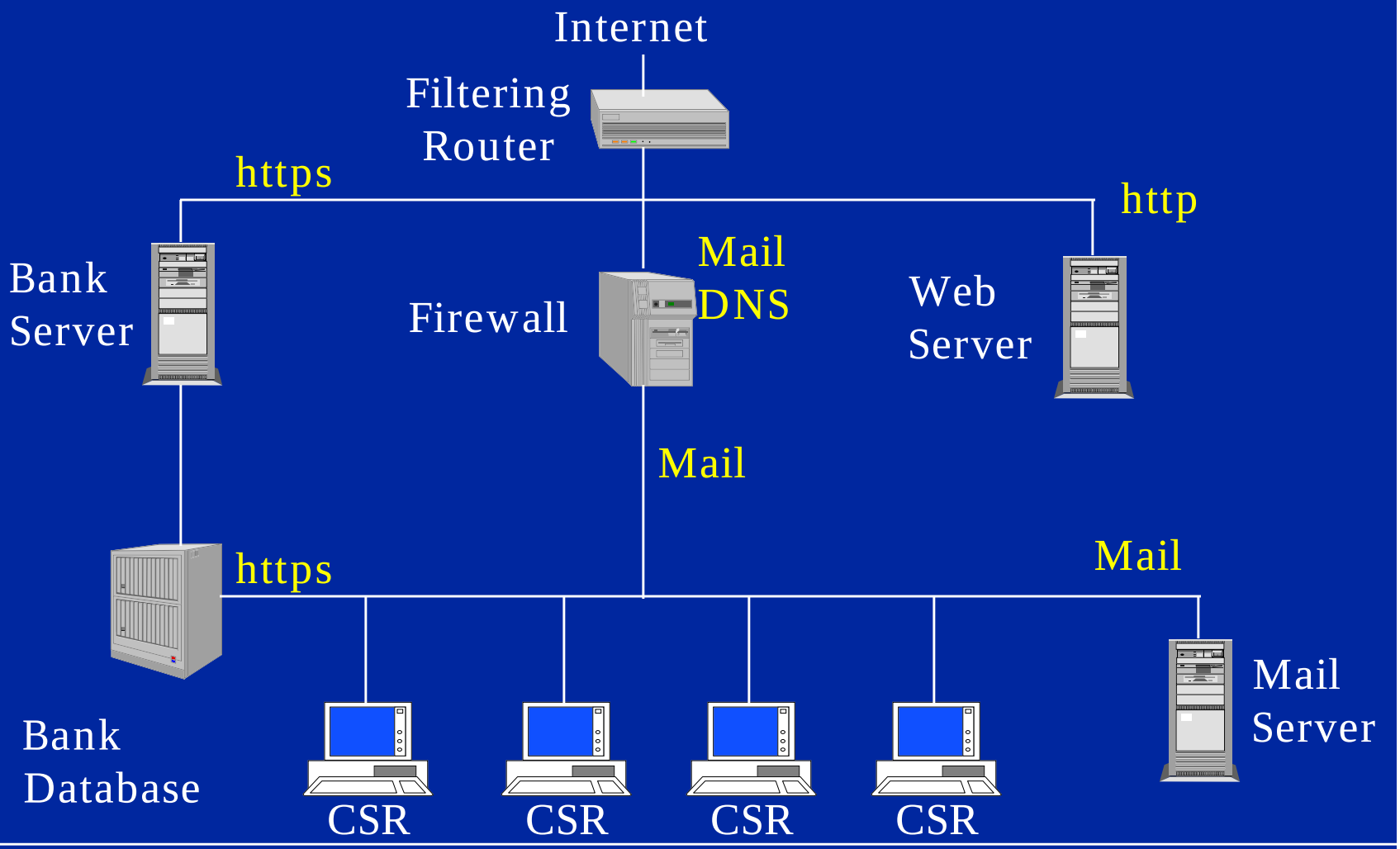
Design Goals

- Web based banking solution
- Fast response time
- Secure
- Easy to administer
- No bank data on the “outside”

Machine Architecture



Data Flow


Internet
Filtering Router
https
http
Bank Server
Firewall
Mail DNS
Web Server
Mail
https
Mail
Bank Database
CSR
CSR
CSR
CSR
Mail Server

Bandwidth Analysis

- How much does the system cost?
- How many customers can the bank support?

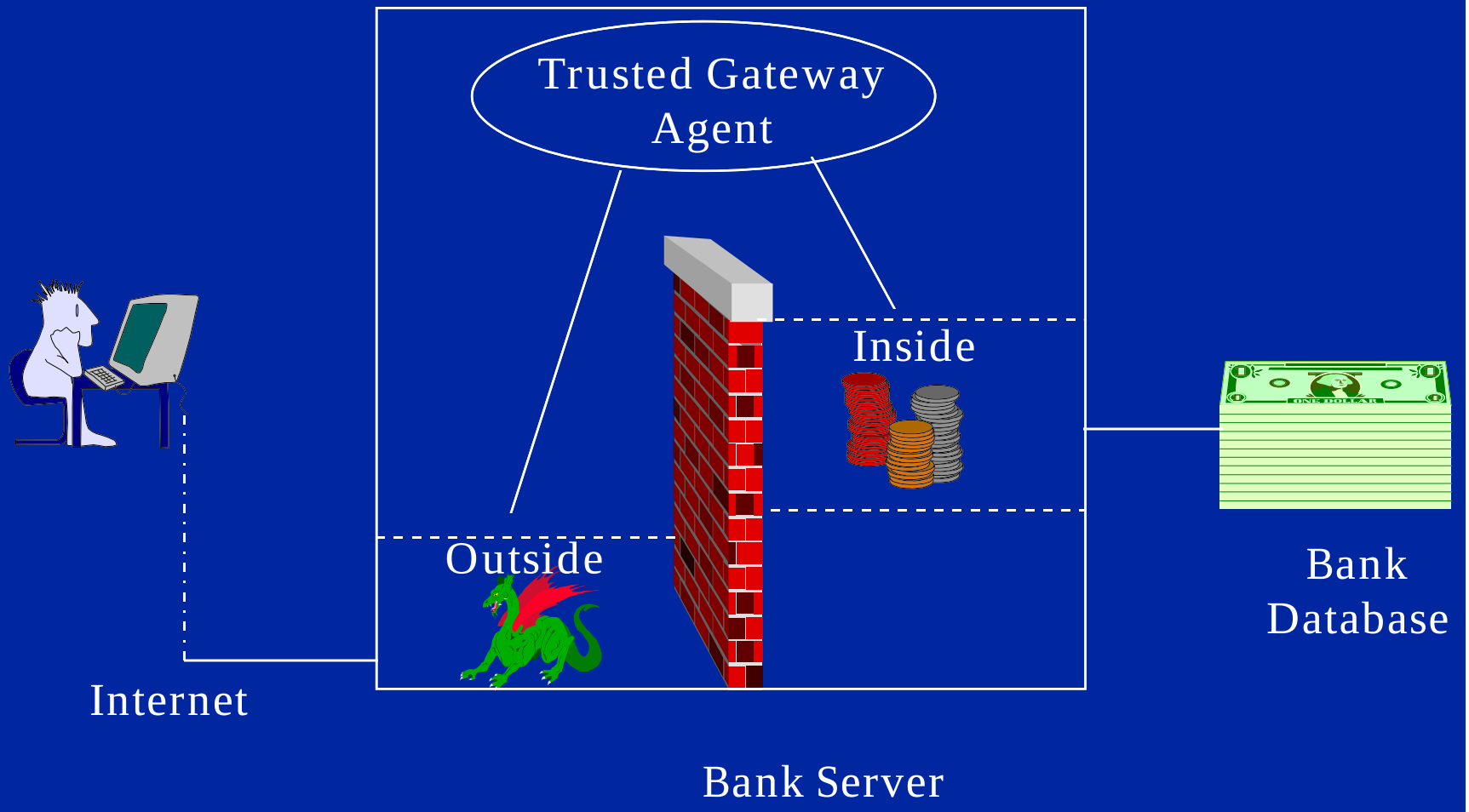
Bank Server

- HP / UX CMW
- Netscape Commerce Server (NCS)
- Verisign certificate
- Bank applications
- No other network services

Bank Server Security

- NCS runs under a pseudo-user account
- NCS runs in a *chroot*-ed environment
- NCS runs at “outside” level
- Bank application run at “inside” level
- Small, easily verified, trusted program connects “outside” (NCS) with the “inside” (bank applications)

Bank Server


Trusted Gateway Agent
Inside
Outside
Internet
Bank Database
Bank Server

Authentication

- Username / password
- Doesn’t use Netscape databases
- Doesn’t use Netscape API (NSAPI)
- Uses Netscape “cookies”
- Cookie changes every connection
- Cookies can time out (go stale)

Potential Attacks

- IP Spoofing
- User name spoofing
- Crack authentication database
- Web server based attacks
- Inside attacks
- Response to attacks